DE MONTFORT UNIVERSITY LEICESTER

+

Academic Support Office
Student and Academic Services

Student Social Media Policy

Created: June 2018 **Author:** Ryan Ward
Originating Directorate: Student and Academic Services
Updated by: Dan Bolger
Approved by: Academic Board
Date of approval: June 2022
Effective date: July 2022
Due for review: June 2023

1. Introduction

1.1. De Montfort University (DMU) recognises the numerous benefits and opportunities that social media presents. We actively use social media to engage with Students and the general public, to celebrate success, communicate research and enhance the University's profile online. Therefore, DMU also actively encourages University Students to make effective and appropriate use of social media channels and to use them to engage in conversations with the DMU community.

1.2. Despite the opportunities presented by social media, there are risks. Social media allows individuals to communicate either in their name or anonymously with a potentially huge audience, and sometimes its informality can encourage us to be less cautious than we would be using other more traditional methods of communication and interaction. Inappropriate use of social media can be damaging to the reputation of the University as well as have a negative impact on Staff and Students.

1.3. This policy is for Students and provides information on the appropriate use of social media when connected, or linked in some way, to their status as a Student of the University, or when directly or indirectly referencing the University in any way.

1.4. This policy works alongside the following separate institutional policies and regulations including but not limited to:

- General Regulations and Procedures Affecting Students, and in particular Chapter 2, Chapter 4 and Chapter 14
- Policy on Dignity and Respect (Students)
- Use of Information Systems Policy
- Freedom of Expression
- Academic Freedom Policy
- DMU's Fitness to Practise procedure
- Data Protection
- Unacceptable Behaviour Policy (dmu.ac.uk)

1.5. The principles of freedom of expression and academic freedom apply to the use of social media; however, the University requires responsible and legal use. (See also the University's *Freedom of Expression and Academic Freedom* policy).

2. Scope

2.1. For the purpose of this policy, the term 'Social Media' is used to describe virtual channels dedicated to live streamed or scheduled uploads, community-based input, interactions, content sharing and collaboration through the building of virtual networks and communities. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation and wikis are among the different types of social media. It also includes any other means of communicating on the internet where members of the public (including Staff or Students) may reasonably access the communication.

2.2. They currently include, but are not limited to, Facebook (and Messenger), Instagram, WhatsApp, Snapchat, TikTok, Twitter, LinkedIn, Reddit, YouTube, Flickr, Pinterest, Clubhouse, WeChat, Weibo, Discord and Google+.

2.3. This policy applies to social media communications made both on public and private forums by Students including those communications which directly or indirectly reference the University. This policy applies to social media uploaded anywhere including off-campus and on personal devices whether to an individual, group or the world. While posts added to public forums can be seen by any member of the public from the date of publication, Students are asked to remember that posts added to private forums (including private messages between two parties) can also be shared publicly by others. Students may be subjected to disciplinary action where they have failed to meet the guidelines in the Student Code of Conduct and all relevant policies referred to in 1.4, in the communication they have posted, even when they believe the forum to be private. There have been a number of high-profile cases in recent years where Students across the country have been disciplined after offensive comments, made on private messaging services such as WhatsApp, were captured and subsequently shared. With this in mind, Students should remember that action can be taken by the University if behaviour failing to meet policy guidelines is identified either publicly or privately.

3. Students' responsibilities

3.1. Students are encouraged to be mindful of how their identity, statements or views appear online and are reminded that current and future employers, and industry contacts may view social media profiles when recruiting to gain information about a candidate's character, personality or employability. Students should therefore bear in mind that any content they publish online may be viewed by a future employer.

3.2. Students registered on professionally accredited programmes should be aware that unacceptable online behaviour may breach the code of conduct of their chosen profession and may have implications for Fitness to Practise.

3.3. It is unacceptable for students on professionally accredited programmes to discuss matters related to the people they may have contact with as part of their placements outside of this setting. Sharing confidential information online can have the potential to be more damaging than sharing it verbally due to the speed at which it can be shared and the size of the potential audience. It is important to remember that although some information may not directly breach an individual's right to confidentiality when anonymised, people may still be identifiable, and this behaviour may breach the Data Protection Act 2018.

3.4. Students are encouraged to review their existing social media accounts and, support can be provided by the University to develop professional social media activity. Advice and guidance is given in Annex A.

3.5. All Students must read and act in accordance with the principles of these guidelines, and regularly check the University's Student regulations and policies (dmu.ac.uk) for any minor updates to documents.

3.6. In addition, it is recommended that Students read and act in accordance with the rules and guidelines set out by individual social media companies and providers.

3.7. Students should check the terms and conditions of a social media account and/or website before uploading material to it; by posting material to social media accounts and/or websites, ownership rights and control of the content may be released. For this reason, it is important to exercise caution in sharing all information, especially where the information, expressly or by implication or innuendo, identifies a third party.

3.8. Students must be aware of the potential impact and permanence of anything posted online. Even if your settings are set to private, other people may share information you have shared with them or there may be information out there from before your settings were changed. Therefore, Students should avoid posting anything:

- they do not wish to be in the public domain.
- which contravenes sections 4, 5 and 6 of this policy.

3.9. Any digital material posted online could reach a wider audience than was expected or intended. Once digital content has been created and shared, there is limited control over its permanence and audience.

3.10. Students should note that they have the right of erasure under the data protection legislation, and that they can request that social media companies remove content concerning themselves. It should be noted that there are circumstances where the social media company can refuse to remove content, for example where they might be used as evidence in legal proceedings.

3.11. Students should note any personal data uploaded onto social media about themselves is normally regarded as being put into the public domain, and therefore has significantly less protection from the data protection legislation.

4. Behaviour and conduct on social media

4.1. Students are personally responsible for what they communicate on or through social media and they must adhere to the standards of behaviour set out in this policy and any related policies, such as Policy on Dignity and Respect Relating to Students and the General Regulations and Procedures Affecting Students.

4.2. Students as users of social media may witness other members of society increasingly using social media for raising complaints and grievances. However, any Students wishing to raise a complaint, report a crime or an incident should do so via the established University channels, e.g. contacting the University Security team or by contacting the Police; Students should contact the University and/or the Police as soon as possible, saving any evidence, e.g. screenshots of social media. Students are advised to bear in mind that sharing details and evidence of a complaint on social media may limit the chances of action taken against any offenders and lead to civil action against the author if the complaint is found to be false.

4.3. Use of social media must not infringe on the rights, or privacy, of other Students or Staff and Students must not make comments or judgements about other Students, Staff or third parties.

4.4. We recommend that permission to share third party material, including all images, photography, text and videos, should be sought and recorded in a tangible format before uploading them to or linking them via social media. Furthermore, where permission is obtained, we recommend such materials should be credited appropriately. Guidance can be obtained from the Library website at Home - DMU - LibGuides at De Montfort University

4.5. The following non-exhaustive list is considered to be of an unacceptable nature and should never be posted:

- Confidential information (which may include research not yet in the public domain, information about fellow Students or Staff or personal matters, non-public or not yet approved documents or information).
- Details of complaints/potential complaints and/or legal proceedings/potential legal proceedings involving the University.
- Personal information about another individual, including contact information, without their express permission.
- Comments posted using fake accounts, made-up names or using another person's name without their consent, including submitting other students' details for surveys, forms and open letters.
- Inappropriate material, including but not limited to images, that is, or may be perceived to be threatening, harassing, discriminatory, illegal, obscene, indecent, defamatory, or hostile towards any individual, group or entity.
- Records, recordings and/or photographs made without the consent of one or more parties concerned and released without a clear public interest case.
- Recordings or any content from University owned DMU Replay material or interactive learning platforms including but not exclusively, Blackboard, Blackboard Collaborate and MS Teams, and online assessments.
- Any other posting that constitutes, or may constitute, a criminal offence.
- Material to prepare to engage in or engage in academic offences.
- Material taken from assessments or exams scripts.
- Any academic work completed by the student in part or full.
- Anything which may bring the University into disrepute or compromise the safety or reputation of colleagues, former colleagues, Students, Staff and those connected with the University.

4.6. Students should be mindful that statements on social media that cause harm to an individual, including to their reputation, or that interfere with an ongoing disciplinary/legal process may create a potential civil claim against the individual making the statement. Furthermore, this may extend to the sharing of statements made by others.

4.7. Students should also be aware that communications on social media are also subject to legislation, which aim to prevent interference with legal proceedings regardless of intent to do so.

4.8. An individual, including the complainant, may undermine proceedings or processes by

publishing information, including imagery, relating to existing or potential complaints and/or legal proceedings. This may be done in the heat of the moment; however, Students should be aware that by doing so they might bring the University into disrepute or compromise the safety of the University community. As such, this conduct may be seen to be of an unacceptable nature, as per paragraph 4.5 above.

4.9. Students, and Student groups, e.g. DSU societies, must take particular care not to state or imply that their views are those of DMU when using social media, nor use the University logo at any time.

4.10. Students should note that extracting data from social media sites for use in projects or research as part of their studies could constitute processing personal data as defined In the General Data Protection Regulations UK and Data Protection Act 2021.

5. Cyber bullying

5.1 The University will not accept any form of bullying or harassment by or of members of the University, Students or stakeholders or visitors, e.g. De Montfort Student Union. Additional information can be found in 3 Chapter 2 (dmu.ac.uk) and the 4 Chapter 2 Annexes (dmu.ac.uk) and the Information Security policies and guidelines.

5.2. The following non-exhaustive list of examples illustrate the types of behaviour, displayed through social media, which the University considers to be forms of cyber bullying:

- Maliciously, negligently or recklessly spreading rumours, lies or gossip
- Intimidating or aggressive behaviour, as perceived by those viewing the social media content.
- Offensive or threatening comments or content, as perceived by those viewing the social media content.
- Posting comments/photos etc. deliberately, negligently or recklessly mocking an individual with the potential to harass or humiliate them, as perceived by those viewing the social media.
- Repeatedly posting comments on social media about an individual or group in an unwanted way, and not complying to requests to desist.
- Accessing any third party's social media either directly or through personal contacts, and using this to post comments about an individual.

5.3. Cyber bullying may also take place via other means of electronic communication such as email, text, instant message, video, audio or images – edited or otherwise.

5.4. Students should be aware that some cases of the above may constitute criminal acts under the Criminal Justice Act (2015), the Communications Act (2003), the Malicious Communications Act (1988) or the Protection from Harassment Act (1997).

6. Students use of official University accounts

6.1. Some Students may contribute to the University's official social media activities as part of their role, for example taking over the Snapchat or Instagram accounts, vlogging, writing blogs or running an official Twitter account, this includes but is not limited to

University sports clubs and societies social media accounts. Students should be aware that while contributing to the University's social media activities they are representing the University and should refer to DMU guidance on acceptable content.

Misuse of official University accounts may lead to suspension and, following a disciplinary committee, may lead to expulsion; Students will not be eligible for readmission to the University at any time in the future as per Chapter 2 of the *General Regulations and Procedures Affecting Students*.

7. Breach of the policy

7.1. If a Student is found to have acted in breach of this policy this may lead to consideration of disciplinary action being taken against them in accordance with Chapter 2 of the *General Regulations and Procedures Affecting Students.*

7.2. Any individual suspected of committing a breach of this policy will be required to cooperate with any investigation in accordance with the disciplinary procedure. Non-cooperation may lead to further disciplinary action in accordance with Chapter 2 of the *General Regulations and Procedures Affecting Students.*

7.3. Students on professionally accredited programmes may also be subject to Fitness to Practise processes as a result of any breach of this policy.

Any individual may be required to remove internet or social media content which is found by the University to be in breach of the policy. Failure to comply with such a request may result in further disciplinary action. Furthermore, internet or social media-based evidence constituting preparation to engage in an academic offence or engagement in an academic offence will be considered under both this policy and the General Regulations.

7.4. Any breach of this policy must be reported in line with DMU's Student Complaints Procedure. In the first instance, any breaches must be brought to the attention of the DMU Security Team by email at security@dmu.ac.uk or by phone on (0116) 257 7642

8. Monitoring

8.1 The University will:

- Ensure this policy, and any changes, is accessible to Staff and Students
- On occasion, provide guidance for Students on how to stay safe online when using social media. Initial guidance is available at Annex A. Further guidance on *Staying Safe Online* is available from ITMS.
- Monitor references to the University on social media and the internet and respond to complaints regarding Student conduct on social media
- Take disciplinary action where inappropriate behaviour is exhibited that affects Students, Staff, the University or members of public in accordance with the University's *General Regulations and Procedures Affecting Students, and in particular Chapters 2 and 14 of those Regulations.*
- Where appropriate refer to the faculty with responsibility for Fitness to Practise processes.

- Annually review and update this policy, where appropriate, and any other associated policy and guidelines and publish details of any changes.

Annex A – How to use social media

How to use social media
Tips and hints on staying safe and managing your reputation

We all recognise the enormous benefits and opportunities that social media presents and we actively encourage our Students to use social media to communicate and keep in touch with latest news and research in their area.

Despite the opportunities, there are risks. Social media allows individuals to communicate with a potentially large audience, and sometimes its informality can encourage us to be less cautious than we would ordinarily be.

These tips are to help you when you are considering posting on social media. They will help you manage your professional reputation and ensure you follow University guidelines and the law.

The Digital Learning and Teaching Team in the Centre for Academic Innovation and Teaching Excellence (CAITE) is able to provide support and guidance for users of various social media technologies.

- **Remember, everything you post online is public**. Once it's out there you lose control of how others might interact with it. Posting anything online (even on closed profiles or private messaging services, like WhatsApp, for example) has the potential to become public, even without your knowledge or consent.

- **Think before you post.** It is important to realise that even the strictest privacy settings have limitations. Once something is online, it can be copied and redistributed. Would you be happy for your family, lecturer or future employer to see it? If not, then it's probably not a good idea to post it. There have been a number of high-profile cases where Students across the country have been disciplined after offensive comments made on private messaging services, like WhatsApp, were captured and subsequently shared.

- **Consider how the content of your messages may appear to others.** Offensive materials, including text, images and video, have the potential to cause serious upset and severely damage your professional and personal reputation. Consider how others may perceive your content. How could a potential employer view the content? **Employers are increasingly checking the digital footprint of potential Staff.** This means looking at old tweets, posts and comments on forums. Will sharing the content result in you falling short of expected standards at University and the law? If so, it could result in the University taking disciplinary action. Don't forget, it can be hard to take something back once it has been shared, copied, or redistributed.

- **Check your privacy settings**. Protect your personal information and that of others that could be misused. Think about who can see your address, telephone number, date of birth and email address. And, definitely don't share your bank details online. Also remember that while you may be sharing the content privately (on your own private profile or in a private forum) others can share that content publicly if it is available.

- **Use Secure Passwords.** Remember to use a secure password and current advice for this is to use a pass phrase of three or more words that you can picture in your head. Never re-use passwords across different websites. Where possible use second factor authentication methods, which may include sites sending an SMS or an authenticator app on your phone. For further information see https://www.getsafeonline.org/protecting-yourself/passwords/

- **Make sure you familiarise yourself with expectations regarding professionalism and confidentiality on your course**, especially if your course is accredited by a professional body. If you breach the code of conduct of a professional body, it is very likely to affect your ability to study, potentially make you subject to fitness to practise proceedings and affect your future career.

- **Be aware of sharing third-party materials**. Do you need permission to share the materials or should you, as a matter of courtesy, contact the party? Make sure you check before posting as infringement of rules could break copyright and/or intellectual property laws.

- **Do not post solutions to assignments on the internet or social media**. If you upload your own answers to coursework or phase test questions then these may be used by others in their own assignments. You could be found guilty of committing the academic offence of collusion.

- **Do not use the internet or social media to incite or facilitate cheating in assessments**. To do so is a breach of this Policy and a disciplinary offence.

- **Finally question everything you read online**. Not everything you read might be completely accurate. Who wrote it? Where did it come from? Does the imagery look poor quality? If you think it looks or sounds inaccurate, it's probably best avoided. Writing and distributing inaccurate statements about people and organisations can be unlawful and lead to legal action.